**ANÁLISE DO PROTOCOLO TCP**

**TRANSFERÊNCIA DE ARQUIVO**

Para a geração das respostas foi utilizada a captura disponível para download no conteúdo online da disciplina.

1. Qual é o número da porta TCP usada pelo computador cliente que está transferindo o arquivo para o servidor “gaia.cs.umass.edu”? Para responder a essa pergunta, é provavelmente mais fácil selecionar uma mensagem HTTP e explorar os detalhes do pacote TCP usado para transportar essa mensagem HTTP, usando os “detalhes da janela de cabeçalho de pacote selecionado”.

Como se trata de uma transferência Web, foi filtrado o protocolo HTTP colocando “http” (sem aspas) no campo “filtro de exibição de pacotes”. Para o arquivo de captura disponível no conteúdo online foram filtrados os pacotes 112 e 130. O pacote 112 foi o envio da solicitação HTTP, e o 130 sua resposta.



Expandindo o “Transmission Control Protocol” em “detalhes do cabeçalho do pacote selecionado”, vemos que o campo “*source port*” (porta origem) possui valor 61384.

Então o número da porta usada pelo computador cliente é 61384.

2. Qual número de porta está sendo utilizado pelo processo da aplicação no servidor “gaia.cs.umass.edu” para o envio e recebimento de segmentos dessa conexão?

Pelo mesmo pacote do segmento utilizado na questão 1 vemos que o capo “*Destination Port*” possui valor 80, então o número da porta usada pelo processo da aplicação no servidor “gaia.cs.umass.edu” é 80.

3. Qual é o número de sequência do segmento TCP SYN que é usado para iniciar a conexão TCP entre o computador cliente e gaia.cs.umass.edu? O que é no segmento que identifica o segmento como um segmento SYN?

O Wireshark provê informações sobre os números de sequência transmitidos por intermédio dos campos:

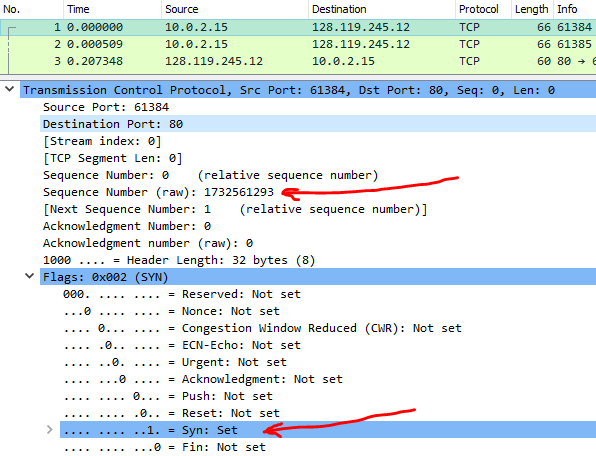
* Sequence Number 🡪 Número de sequência relativo da transmissão, como se o primeiro número de sequência fosse 0.
* Sequence Number (raw) 🡪 Número de sequência bruto do TCP (número de sequência real negociado pelo TCP).

Na filtragem feita pelo protocolo HTTP para responder à questão 1 vimos que as mensagens HTTP são trocadas entre os hospedeiros com endereços IP 10.0.2.15 (computador local) e 128.119.245.12 (servidor gaia.cs.umass.edu).

Limpando o campo “filtro de exibição de pacotes” podemos perceber que o primeiro pacote trocado entre esses hospedeiros foi o pacote nº 1, sendo ele o início da solicitação de conexão.

Conforme pode ser observado na figura o segmento possui o flag “SYN” com valor 1, indicando que se trata de um segmento de estabelecimento de conexão.

No mesmo segmento o campo de cabeçalho “Sequence Number (raw)” possui valor 1732561293, indicando que o número de sequência estabelecido pelo cliente é 1732561293.



4. Qual é o número de sequência do segmento SYN/ACK enviado por “gaia.cs.umass.edu” para o computador cliente em resposta ao SYN? Qual é o valor do campo Confirmação no segmento SYN/ACK? Como gaia.cs.umass.edu determinou esse valor? O que é no segmento que identifica o segmento como um segmento SYN/ACK?

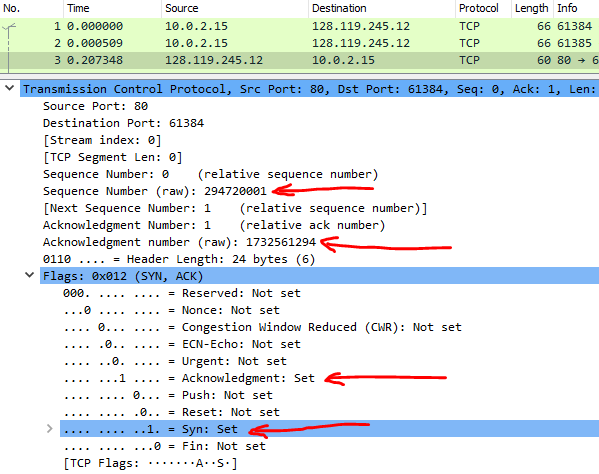
A resposta ao pedido de solicitação de conexão do pacote 1 vem no pacote 3.

O campo de cabeçalho “Sequence Number (raw)” possui valor 294720001, indicando que o número de sequência estabelecido pelo servidor é 294720001.

O campo de cabeçalho “Acknowledgment number (raw)” possui valor 1732561294, que é o número de confirmação enviado pelo servidor. Esse valor indica o próximo byte aguardado em relação ao último byte enviado.

Como o segmento enviado pelo cliente possuía número de sequência 1732561293, o servidor confirmou seu recebimento enviando esse mesmo número somado de 1 como número de confirmação.

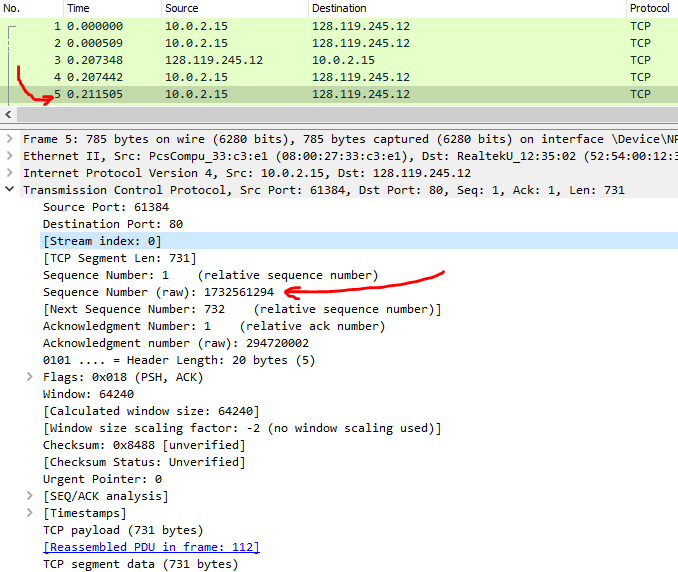
Esse segmento é um segmento SYN/ACK porque é um segmento que está sendo utilizado no estabelecimento da conexão (flag SYN com valor 1) e porque carrega um valor de confirmação válido (flag Acknowledgment com valor 1).



5. Identifique o primeiro segmento TCP que envia dados ao servidor “gaia.cs.umass.edu”. Dica: haverá no segmento uma indicação “TCP segment data” indicando que o segmento carrega dados. Qual é o número de sequência desse segmento TCP?

O primeiro segmento que carrega dados TCP está contido no pacote nº 5.

Seu número de sequência de acordo com o campo de cabeçalho “Sequence Number (raw)” é 1732561294. Esse era o valor esperado uma vez que é o valor passado pelo servido como número de confirmação.



6. Considere o primeiro segmento contendo dados como o primeiro segmento na conexão TCP. Qual é o tamanho de cada um dos cinco primeiros segmentos TCP?

Os 5 primeiros segmentos TCP contendo dados que foram enviados foram os pacotes 5, 7, 18, 29 e 37.

Podemos observar a quantidade de dados que cada segmento carrega expandindo o “Transmission Control Protocol” em “detalhes do cabeçalho do pacote selecionado”. Nele tanto “TCP Segment Len” quanto “TCP payload” informam a quantidade de bytes transportada pelo segmento TCP.

Para obter o tamanho de cada segmento TCP devemos somar o tamanho do cabeçalho à quantidade de dados. O tamanho do cabeçalho é dado pelo campo de cabeçalho “HLEN”, que informa a quantidade de palavras de 4 bytes (32 bits) que compõem o cabeçalho.

Assim:

PACOTE 5:

“HLEN” = 5 (20 bytes) e “TCP Segment Len” = 731.

Tamanho total = 751

PACOTE 7:

“HLEN” = 5 (20 bytes) e “TCP Segment Len” = 14600.

Tamanho total = 14620

PACOTE 18:

“HLEN” = 5 (20 bytes) e “TCP Segment Len” = 18168.

Tamanho total = 18188

PACOTE 29:

“HLEN” = 5 (20 bytes) e “TCP Segment Len” = 16384.

Tamanho total = 16404

PACOTE 37:

“HLEN” = 5 (20 bytes) e “TCP Segment Len” = 16384.

Tamanho total = 16404

7. Quais são os números de sequência dos cinco primeiros segmentos na conexão TCP? Em que momento (time) cada segmento foi enviado? Quando o ACK de cada segmento foi recebido?

PACOTE 5

Nº sequência: 1732561294

Time: 0,211505

Como o pacote 5 contém 731 bytes de dados, é aguardado nº de confirmação 1732562025.

O ACK foi recebido pelo pacote nº 6, com time 0,211800 (ACK=1732562025).

PACOTE 7

Nº sequência: 1732562025

Time: 0,217574

Como o pacote 7 contém 14600 bytes de dados, é aguardado nº de confirmação 1732576625.

Foram recebidos vários ACKs confirmando chegadas parciais dos dados do segmento, sendo o último deles no pacote nº 17, com time 0,218412 (ACK=1732576625).

PACOTE 18

Nº sequência: 1732576625

Time: 0,218496

Como o pacote 18 contém 18168 bytes de dados, é aguardado nº de confirmação 1732594793.

Foram recebidos vários ACKs confirmando chegadas parciais dos dados do segmento, sendo o último deles no pacote nº 32, com time 0,219223 (ACK=1732594793).

PACOTE 29

Nº sequência: 1732594793

Time: 0,219073

Como o pacote 29 contém 16384 bytes de dados, é aguardado nº de confirmação 1732611177.

Foram recebidos vários ACKs confirmando chegadas parciais dos dados do segmento, sendo o último deles no pacote nº 45, com time 0,219614 (ACK=1732611177).

PACOTE 37

Nº sequência: 1732611177

Time: 0,219411

Como o pacote 37 contém 16384 bytes de dados, é aguardado nº de confirmação 1732627561.

Foram recebidos vários ACKs confirmando chegadas parciais dos dados do segmento, sendo o último deles no pacote nº 58, com time 0,220117 (ACK=1732627561).

8. Considerando os cinco primeiros segmentos de dados explorados na questão anterior, algum segmento foi enviado antes do recebimento da confirmação informando o recebimento completo do segmento anterior?

Podemos perceber que:

O segmento com nº de sequência 1732594793 (pacote nº 29) foi enviado no tempo 0,219073, mas a confirmação do segmento anterior chegou somente no tempo 0,219223 (pacote nº 32).

O segmento com nº de sequência 1732611177 (pacote nº 37) foi enviado no tempo 0, 219411, mas a confirmação do segmento anterior chegou somente no tempo 0, 219614 (pacote nº 45).

Dessa forma são enviados segmentos de dados antes que a confirmação do segmento anterior seja entregue.

9. Qual é a quantidade mínima de espaço de buffer disponível anunciado pelo servidor durante todo o processo de transferência do arquivo?

O servidor anuncia seu espaço disponível em buffer por intermédio do campo de cabeçalho “Window”. Observando esse campo em todos os pacotes que chegaram do servidor pode-se determinar o menor tamanho da janela.

DICA: Você pode aplicar um filtro para listar somente os pacotes enviados pelo servidor. Esse filtro é o “ip.src”. Se o endereço IP do servidor for 128.119.245.12, digite “ip.src==128.119.245.12” (sem as aspas) no campo “filtro de exibição de pacotes”. Depois clique sobre o primeiro pacote e vá descendo com a seta para baixo do teclado, enquanto observa o valor o campo “Window”.

O menor valor encontrado para o campo “Window” é 164 (pacote 108).

10. Existem segmentos retransmitidos?

Aplicando o filtro “ip.src” em conjunto com o filtro “ip.dst” é possível filtrar somente as mensagens de um hospedeiro específico para outro. Por exemplo, para filtrar as mensagens enviadas de 10.2.0.15 para 128.119.245.12 pode ser utilizado o filtro “ip.src==10.0.2.15 and ip.dst==128.119.245” (sem aspas). Utilize esse filtro para mostrar somente as mensagens enviadas de seu computador para o servidor.

O Wireshark provê informações sobre os números de sequência transmitidos por intermédio dos campos:

* Sequence Number 🡪 Número de sequência relativo da transmissão, como se o primeiro número de sequência fosse 0.
* Sequence Number (raw) 🡪 Número de sequência bruto do TCP (número de sequência real negociado pelo TCP).
* Next Sequence Number 🡪 Qual deverá ser o número de sequência enviado pelo próximo segmento, considerando números de sequência relativos.

Analisando o pacote 5, por exemplo, podemos observar que o campo “Sequence Number” possui valor 1, e que o campo “Next Sequence Number” possui valor 732. Então é esperado que o próximo segmento enviado possua número de sequência 732.

Analisando o pacote 7, segmento enviado posteriormente ao segmento 5, vemos que o campo “Sequence Number” possui valor 732, indicando que o pacote 7 não é uma retransmissão.

Fazendo essa análise pata todos os segmentos enviados do computador para o servidor não foram encontradas retransmissões.